Claims 1-7, 10 and 11 have been rejected under 35 USC 103(a) as unpatentable over a combination of Goldman ' 936 in view of Indeck '461. Claims 8, 9 and 12 have been indicated to be allowable if rewritten in independent form with all limitations of the base and intervening claims.

The 35 USC 112 Rejection of Claims 15, 19 and 21

The terminology "DeLand enabled scanner/card reader" refers to a card scanner or card reader which has been designed and constructed to verify the authenticity of magnetic stripe cards pursuant to the teaching of U.S. Patent 6.,098,881 issued to DeLand, Jr. et al. The DeLand patent is referenced at page 2, line 33 through page 3, line 3, of the specification as providing enabling technology for authenticating mag stripe cards. The DeLand technology incorporates technology disclosed in a series of patents issued to Ronald S. Indeck listed on page 2, lines 12-19 of the specification. The authentication is generally performed by reading or sensing microstructural information of the magnetic stripe medium and comparing that information to prerecorded and stored microstructural information. The undersigned does not know whether "DeLand" is a trademark; however, the term is not used as a trademark in the application.

The referenced DeLand and Indeck patents describe the card authentication technology in a way such as to enable one skilled in the art to make and/or use scanners/card readers capable of authenticating card readers by sensing magnetic medium microstructure.

For the foregoing reasons, it is respectfully requested that the rejection of Claims 15, 19 and 21 under 35 USC 112 be withdrawn.

The 35 USC 103 Rejection of Claims 1-7, 10 and 11 based on Goldman v. Indeck '462

The Examiner cites Goldman as teaching a magnetic stripe identity card on which is recorded card uniqueness data derived by scanning a card . This scanned data include variations in translucency peculiar to the material of a given card unit and also variations introduced by printing on the card, such as photos and printed personal information. Goldman further teaches that this uniqueness data identifying the card is recorded or stored on the magnetic strip of the card.

The Examiner concedes that Goldman fails to teach a second reference data element representative of a biometric aspect of the card holder and of the digital data storage medium being a magnetic stripe.

To supply this missing teaching, the Examiner relies upon Indeck '462. The Examiner states that Indeck teaches, at column 8, lines 30-35, the use of a secondary security check in the form of a human fingerprint and that it also teaches the recording of the magnetic fingerprint of the mag stripe card.

The Examiner concludes that one of ordinary skill would have found it obvious to encode and record the uniqueness of the magnetic stripe itself onto the magnetic stripe rather than data derived from some other region of the card as suggested by Goldman. Furthermore, the Examiner proposes that it would have been obvious to modify Goldman so as to utilize a biometric aspect to be stored on the magnetic stripe for providing unique and distinctive identification of the card holder.

Issue is respectfully taken with the Examiners' remarks regarding the teaching of Indeck and the proposed modification of Goldman in view of Indeck.

In the rejection, the Examiner relies upon Indeck's teaching at Column 8, lines 30-35 as the basis for incorporating a stored biometric aspect on the mag stripe recording medium of the Goldman card.

In fact, Indeck '462 supplies no such teaching. The language referred to by the Examiner bears quoting in full here:

> *"This is especially true if a system utilizes not only the magnetic fingerprint of a particular passcard, but also utilizes a secondary security check such as a picture ID, human fingerprint, hologram (presently imprinted on credit cards), or such other methodology which would thereby render the passcard system virtually impregnable."*

The Indeck '462 language contains no more that a passing referenc to th use of a human fingerprint as a "secondary security check". Furthermore, the suggested use of a human fingerprint is lumped together with other "secondary security" checks such as a picture ID or a hologram, among still other methodologies.

Indeck '462 fails to explain how such as secondary security check is to be applied or implemented. In particular, Indeck nowhere teaches nor suggests that a human fingerprint or other biometric aspect of the card user be recorded in digitally readable form on the magnetic stripe of the card along with other card uniqueness data. Indeck does not suggest that the secondary security check be electronically recorded, whether on the card or elsewhere, and does not even suggest that the fingerprint be printed on the card. In fact, Indeck '462 is entirely silent as to how the secondary security check, including a human fingerprint, is to be used to supplement the "magnetic fingerprint" of a particular pass card. There is no teaching or suggestion made by Indeck to lead one of ordinary skill in the art to this applicant's claimed invention.

Given that the combination of references relied upon by the Examiner do not teach the recording of biometric data on the data storage medium of the card, the Examiner's position and consequent rejection can only be based on a hindsight reconstruction of the prior art in light of this applicant's disclosure.

The Applicant's Claimed Invention

The applicant's invention and, in particular, the invention of Claim 1, is neither taught nor suggested by the Examiner's proposed combination of Goldman and Indeck '462, nor by any other art of record.

This applicant's invention differs from any combination of Goldman and Indeck '462 in that the card encoded according to this applicant's invention provides reference data which verifies the authenticity of the physical card presented at a transaction site and also verifies the identity of the person presenting the same at that same transaction site.

Goldman and Indeck '462, however these two references are combined, can do no more than provide stored uniqueness data to permit authentication of the physical card presented at the transaction site.

This dual verification can be done to a high degree of reliability by digitally storing reference data including both the card identifying data and user biometric data, and making the stored reference data available at a card transaction location where the reference data can be electronically compared by an appropriate card reader against live card and biometric data acquired in the field from the card presented and from the live person presenting the card. This field acquisition of live data can be made, for example, by a suitably configured card reader combined with a biometric scanner at the transaction site.

Further yet, neither of the references suggest the encoding of the card data and biometric data into a single encoded data element for still greater security, as in Claim 2, such that neither the card data nor the biometric data can be retrieved without access to a decoding algorithm.

The Amended Claims

Claim 1 has been amended to more clearly specify the invention, and as amended, Claim 1 is believed to be allowable over the art of record. Dependent Claims 2-7, 10 and 11 are believed to be allowable therewith. New claims 24 through 40 have been added and are believed to be also allowable in view of the art of record and the preceding remarks.

Review and reconsideration of the application in light of the foregoing remarks and accompanying amendments is respectfully requested. A Notice of Allowability is believed to be in order and such action is earnestly solicited.

Respectfully submitted,

Dated: June 13, 2003

Natan Epstein
Registration No. 28,997
Attorney for Applicant